



RECEIVED

JAN 19 1993

FCC MAIL ROOM

January 12, 1993

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs, and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic

No. of Copies rec'd
List ABCDE

Orig + 4

interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXC's were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LEC's should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and education services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

A handwritten signature in cursive script, appearing to read "Stella Goulet".

Stella Goulet
Director, Facilities Services



120 LONG RIDGE ROAD, P.O. BOX 1355, STAMFORD, CT 06904-1355

RECEIVED

JAN 19 1993

FCC MAIL ROOM

January 10, 1993

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

No. of Copies rec'd
List ABCDE

044

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

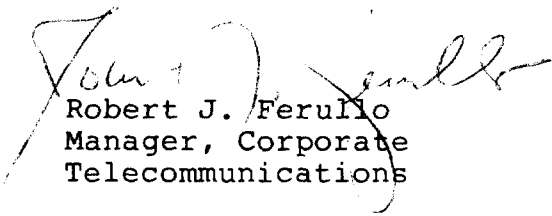
However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,



Robert J. Ferullo
Manager, Corporate
Telecommunications

AM

TEXTRON Marine Systems

Textron Marine Systems/
Division of Textron Inc.

RECEIVED
JAN 19 1994
FCC MAIL ROOM

6600 Plaza Drive
New Orleans, LA 70127-2584
504/245-6600

January 12, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

No. of Copies rec'd
List ABCDE

024

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

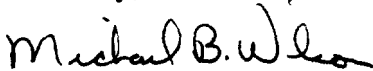
However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

A handwritten signature in cursive script that reads "Michael B. Wilson".

Michael B. Wilson
Manager, Information Services
and Special Projects



Phoenix Home Life

January 13, 1994

Mr. William Caton
Acting Secretary
Federal Communications Commission
Common Carrier Bureau
1919 M Street NW
Washington, DC 20554

RECEIVED

JAN 19 1994

FCC MAIL ROOM

Re: FCC Docket 93-292 Toll Fraud

Dear Mr. Caton:

I am writing in support of the proposals included in FCC Docket 93-292 on Toll Fraud. Our company has experienced loss through toll fraud and we firmly believe that the liability should be shared among the customer, the network carrier, and the PBX manufacturer. We believe the network carrier has liability and responsibility because they have the monitoring tools available and the point of view to see fraud take place, and they have the capability of implementing both monitoring and control measures which would lessen the risk of massive violation. We believe the equipment manufacturers have liability because they can improve the security controls on their equipment and improve the training they offer to plan and implement schemes of security. They also have the capability of providing monitoring tools and training to support customer efforts.

Thank you for your attention.

Sincerely,



Jeffrey M. Lewis

No. of Copies rec'd
List ABCDE

Quigley

January 11, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

RECEIVED
JAN 19 1994
FCC MAIL ROOM

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE

Quigley

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

A handwritten signature in black ink, appearing to read "Joe R. Neuberry Jr.", written in a cursive style.

January 11, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

RECEIVED

JAN 19 1994

FCC MAIL ROOM

Merck & Co., Inc.
One Merck Drive
P.O. Box 100
Whitehouse Station NJ 08889-0100
Tel 908 423 1000



Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE

Aug.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXCs and LECs to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,



Kathleen M. O'Grady
Facilities Analyst
Information Technology Services



RECEIVED

JAN 19 1994

FCC MAIL ROOM

January 11, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As the person responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their system. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day. As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXCs.

No. of Copies rec'd
List ABCDE

Orig

-PAGE 2-

Mr. William F. Canton

January 11, 1994

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXCs and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

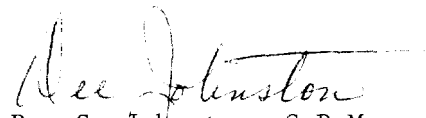
The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only "hack" to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Yours very truly,

O'SULLIVAN CORPORATION


Dee S. Johnston, C.P.M.
Vice President, Purchasing

DSJ/kms

RECEIVED

JAN 19 1994

FCC MAIL ROOM

January 11, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd _____
List ABCDE _____

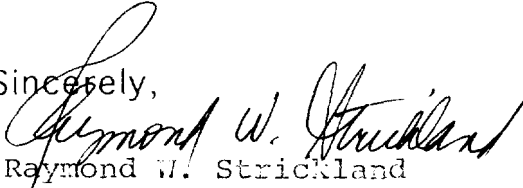
CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure that if we all work together we can and will make a positive impact on this problem.

Sincerely,

Raymond W. Strickland
Telecommunications Manager
Superior Court of D.C.

January 10, 1993

RECEIVED

JAN 19 1993

FCC MAIL ROOM

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

No. of Copies rec'd _____
List ABCDE _____

Rudolph/Libbe Inc.

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

Rudolph/Libbe Inc.

Jane Zautner

Jane Zautner

Telecommunications Manager



RECEIVED

JAN 19 1994

FCC MAIL ROOM

January 12, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

Re: CC Docket No. 93-292

Dear Mr. Canton:

I am a telecommunications manager who is responsible for my company's telecommunications systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard, MCI Detect, and AT&T Netprotect) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login ID's, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all

No. of Copies rec'd
List ABCDE

One

vendor passwords will meet minimum requirements regarding length, change schedule, and alphanumeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s), and IXC(s) involved.

Toll fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,



Thomas J. Frenette
Network Systems Manager



14 Pacella Park Drive
Randolph, MA 02368
(617) 961-4000
Telex: 940388
Facsimile: Grp III (617) 963-2913

DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 19 1994

FCC MAIL ROOM

January 10, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

No. of Copies rec'd
List ABCDE
One

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

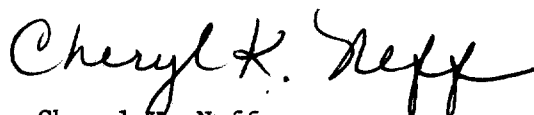
However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

A handwritten signature in cursive script that reads "Cheryl K. Neff".

Cheryl K. Neff
Telephone Operations Manager



DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 19 1994

FCC MAIL ROOM

DEPARTMENT OF TELECOMMUNICATIONS SYSTEMS

January 13, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

RE: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunication professional who is responsible for George Washington University's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard/TM, MCI Detect/TM, and AT&T Netprotect/TM) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including

No. of Copies rec'd
List ABCDE

Aug.

those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment;
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment; and
- IXC(s) and LEC(s) to offer detection, notification, prevention, and educational services.

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,



Robert L. Longshore
Director, Telecommunications
George Washington University

**ARCH
MINERAL
CORPORATION**

CITYPLACE ONE
ST. LOUIS, MISSOURI 63141-7056
(314) 994-2700

RECEIVED

JAN 11 9 1994

FCC MAIL ROOM

January 12, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street, N.W.
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we do not control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions but also by the information, services, and equipment provided IXC's, LEC's, and CPE's, the law should reflect that. It is preposterous to think that the IXC's, LEC's, and CPE's, who all have a very important part in this issue, have absolutely no legal obligations to warn customers and, therefore, no real incentive to stop fraud.

CPE's should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPE's ship equipment without default passwords which are well-known within the hacker community. Passwords should be created during the installation of the equipment with the customers' full knowledge. CPE's should be required to include safety-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car, not an adjunct that you have to purchase later.

While the programs offered by IXC's, such as MCI Detect, AT&T NetProtect, and Sprint Guard have broken new ground in relation to preventing toll fraud, they still do not do enough. Some of these services are too expensive for smaller companies, and the educational information is superficial. I am also encouraged by the monitoring activity that the IXC's have recently begun under some service

No. of Copies rec'd
List ABCDE

One

plans, but again, it is neither consistent nor sufficient. Monitoring by the IXC's should be a part of the basic interexchange service offerings as all companies, large and small, are vulnerable to toll fraud. If the IXC's were monitoring all traffic, there would not be any cases of toll fraud for periods longer than a day.

As hackers begin new methods of breaking into systems by using local lines instead of 800 numbers, the LEC's should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud, not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there would not be a toll fraud problem. While it is the hacker who breaks into the systems and sells the information, it is the call-sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Very truly yours,



Donald B. Staten
Manager, Technical Services

DBS/djc